Exercise 1: nslookup

Use the nslookup command from the "Tools of the Trade" and answer the following questions:

1. Which is the IP address of the website www.koala.com.au? In your opinion, what is the reason of having several IP addresses as an output?

   Koala has two IPv4 addresses :

   - 104.18.60.21
   - 104.18.61.21

   and two IPv6 addresses:

   - 2606:4700:30::6812:3c15
   - 2606:4700:30::6812:3d15

   One of the reasons why Koala.com.au would have several IP addresses is because it wants to provide backup servers when one of their primary servers go down/fails. By having multiple IP addresses, the developers can also halt one of the servers for maintenance and efficiently distribute incoming network traffic, reducing the load it has on each individual server. These IP addresses can also be held at different locations, providing users who access the website greater speeds if they happen to connect within those areas.

2. Find out name of the IP address 127.0.0.1. What is special about this IP address?

   The name of this address is localhost. This IP address is special as it only communicates within your own device and not to other networks. It does this as the TCP/IP stack reroutes any messages sent to the destination of 127.0.0.1. back to the receiving end of the TCP/IP stack.

Exercise 2: Use ping to test host reachability

Are the following hosts reachable from your machine by using ping:

- www.unsw.edu.au -> reachable
- www.getfittest.com.au -> unreachable
- www.mit.edu -> reachable but did not return packet
- www.intel.com.au -> reachable
- www.tpg.com.au -> reachable
- www.hola.hp -> unreachable, does not exist
- www.amazon.com -> reachable
- www.tsinghua.edu.cn -> reachable
- www.kremlin.ru -> reachable but did not return packet
- 8.8.8.8 ->reachable

If you observe that some hosts are not reachable, then can you explain why? Check if the addresses unreachable by the ping command are reachable from the Web browser.

For all the unreachable hosts in the list above, only www.hola.hp and www.getfittest.com.au were also not reachable from the web browser. This is because the host name did not exist and so it was not reachable by ping. For the hosts ww.mit.edu and www.kremlin.ru ping was able to reach these hosts, however there was 100% packet loss as the packets sent over the ping were not returned. This may be due to firewall settings on the host side.

Exercise 3: Use traceroute to understand network topology

Note: Include all traceroute outputs in your report.

1. Run traceroute on your machine to www.columbia.edu . How many routers are there between your workstation and www.columbia.edu ? How many routers along the path are part of the UNSW network? Between which two routers do packets cross the Pacific Ocean? Hint: compare the round trip times from your machine to the routers using ping.

   There are 22 routers between my workstation and www.columbia.edu.

   There are 5 routers along the path that are a part of the UNSW network:

   - cserouter1-server.cse.unsw.EDU.AU (129.94.242.251)
   - 129.94.39.17
   - libudnex1-vl-3154.gw.unsw.edu.au
   - libcr1-po-5.gw.unsw.edu.au
   - unswbr1-te-2-13.gw.unsw.edu.au

   The packet crosses the Pacific Ocean between router 7 and 9 as you can see from the address it goes from NSW to SEA (Seattle, USA)

   - 7 et-1-3-0.pe1.sxt.bkvl.nsw.aarnet.net.au (113.197.15.149) 2.019 ms 2.508 ms 2.497 ms
   - 9 et-2-1-0.bdr1.a.sea.aarnet.net.au (113.197.15.201) 146.682 ms 146.634 ms 146.578 ms

2. Run traceroute from your machine to the following destinations:
   (i) www.ucla.edu (ii) www.u-tokyo.ac.jp and (iii) www.lancaster.ac.uk . At which router do the paths from your machine to these three destinations diverge? Find out further details about this router. (HINT: You can find out more about a router by running the whois command: whois router-IP-address). Is the number of hops on each path proportional the physical distance? HINT: You can find out geographical location of a server using the following tool - http://www.yougetsignal.com/tools/network-location/

   138.44.5.0 is the last router before the three paths diverge. This router is still a part of AARNet (Australian Academic and Research Network) and is located within South Australia.

   The number of hops on each path are not proportional to the physical distance as there was 14 hops from to UCLA however there were more hops to U-tokyo (15 hops) despite there being a larger physical distance. In addition to this Lancaster, which is almost double the distance of UCLA, only has 18 hops.

3. Several servers distributed around the world provide a web interface from which you can perform a traceroute to any other host in the Internet. Here are two examples:
   (i) http://www.speedtest.com.sg/tr.php and (ii) https://www.telstra.net/cgi-bin/trace . Run traceroute from both these servers towards your machine and in the reverse direction (i.e. from your machine to these servers). You may also try other traceroute servers from the list at www.traceroute.org . What are the IP addresses of the two servers that you have chosen. Does the reverse path go through the same routers as the forward path? If

you observe common routers between the forward and the reverse path, do you also observe the same IP addresses? Why or why not?

http://www.speedtest.com.sg/tr.php (IP address is 202.150.221.170)

www.telstra.net/cgi -bin/trace (IP address is 203.50.5.178)

The paths are different e.g. Telstra follows 11 routers from the path to my machine whilst my path to Telstra follows 13 routers (Speedtest.com 9 to 14). This is because the hosts generally have multiple routers to their destination to ensure that there are multiple methods of accessing their website in case one of the routers in the paths go down. The packets travel along these different paths as Linux traceroute implements UDP transfer protocol and so they don't contain the information on following the same path (creating asymmetric routing).

The IP addresses are different as each router can have different IP addresses. As such the packets sent from the traceroute between my local machine and these host websites can travel along these different IP addresses. Having multiple addresses allows for load-balancing and so the packets are distributed depending on incoming network traffic.

Exercise 4: Use ping to gain insights into network performance

1. For each of these locations find the (approximate) physical distance from UNSW using Google Maps and compute the shortest possible time T for a packet to reach that location from UNSW. You should assume that the packet moves (i.e. propagates) at the speed of light, 3×10^8 m/s. Note that the shortest possible time will simply be the distance divided by the propagation speed. Plot a graph where the x-axis represents the distance to each city (i.e. Brisbane, Manila and Berlin), and the y-axis represents the ratio between the minimum delay (i.e. RTT) as measured by the ping program (select the values for 50 byte packets) and the shortest possible time T to reach that city from UNSW. (Note that the y-values are no smaller than 2 since it takes at least 2*T time for any packet to reach the destination from UNSW and get back). Can you think of at least two reasons why the y-axis values that you plot are greater than 2?

   University of Queensland is 952.4km away
   Therefore shortest possible time is $952.4 \times 10^3 / 3 \times 10^8 = 0.00317$ seconds

   De La Salle University is 6266 km away
   Therefore shortest possible time is $6266 \times 10^3 / 3 \times 10^8 = 0.021$ seconds

   Berlin Institute of Technology is 16095 km away
   Therefore shortest possible time is $16095 \times 10^3 / 3 \times 10^8 = 0.054$ seconds

   One of the reasons why the y-axis values are greater than two is because they cannot travel at the rate of 3 x 10^8 m/s as this is the speed of light in a vacuum. In addition to this, the packet may experience a multitude of network delays such as queueing delays due to high traffic intensity.

2. Is the delay to the destinations constant or does it vary over time? Explain why.

   The delay to the destinations vary over time as it is dependent on the network path each packet takes and the network traffic each router in the path is experiencing. For example if there is a lot of network traffic, delay is increased due to increased queueing in the buffer, or if the packet takes a different route, the delay may also be increased if it has to travel through more links.

3. Explore where the website for www.epfl.ch is hosted. Is it in Switzerland?

   The website is being hosted in Australia as (from traceroute) it only takes 1-2 milliseconds for packets to send to host. This is because the website is cached within a server in Australia and this is shown by a whois lookup where it says the server is being hosted by Cloudfare.

4. The measured delay (i.e., the delay you can see in the graphs) is composed of propagation delay, transmission delay, processing delay and queuing delay. Which of these delays depend on the packet size and which do not?

   Only transmission and processing delay depend on packet size. Transmissions involve sending the packet onto the link and as such depends on the packet length divided by the bandwidth of the link. Processing delays depend on packet size as it checks if the packet has any errors. It does so by computing the bits and comparing it to the packet header.